

VVPAT Requirements

John P. Wack

April 20, 2004

Overview

- March '05 Summary
- Comments Received
- Major Issues
- Conclusions
- Requirements Summary
- Discussion

March '05 Summary

- Presented overview, high-level discussion of major issues
- Summary of enacted State VVPAT legislation
- Draft VVPAT requirements
 - Incorporated some State-based requirements
 - Reviewed CA and draft IEEE standards
 - NIST added other requirements

Overview of Comments

- Comments received
 - TGDC
 - Vendors
 - Various voting officials and community
- Comments were evenly distributed
- Common thread – some requirements too specific, design-oriented

Major Issues

- Privacy
 - Sequential storage of paper records affects privacy
 - Many pros/cons to different paper formats
 - Some vendors using different printers and paper
- Accessibility
 - Some requirements may be difficult to meet
 - Accessibility of VVPAT requires more analysis

Conclusions

- VVPAT is new, requires study, benchmarks, new procedures, approaches for accessibility
- Mandates have drawback of not permitting time for evolution of best approaches
- Vendors at a disadvantage but at same time are responding with interesting approaches
- Usability for voters and election officials very high priority
- NIST to issue technology-independent, performance-driven requirements

Overview of Requirements

- Usability, accessibility emphasized, requirements are largely from new Human Factors section (2.2.7)
- Voter privacy of stored records required
- Record formats reflect goal to make records more useful in ballot audits

Core VVPAT Requirements

1. **The voting station shall print and display a paper record of the voter's ballot choices prior to the voter making the ballot choices final**
2. **All usability requirements from section 2.2.7 shall apply to voting stations with VVPAT**
3. **All accessibility requirements from section 2.2.7 shall apply to voting stations with VVPAT**
4. **The voting station shall allow the voter to approve or spoil the paper record**
5. **The voter's privacy and anonymity shall be preserved during the process of recording, verifying, and auditing ballot choices**
6. **The voting station's ballot records shall be structured and contain information so as to support highly precise audits of their accuracy**
7. **The voting station equipment shall be secure, reliable, and easily maintained**

1: Print and Display a Paper Record

6.0.2.1.1 - The paper records shall constitute a complete record of ballot choices that can be used in audits of the accuracy of the voting station's electronic records, in audits of the election results, and in full recounts.

6.0.2.1.2 - The paper record shall contain all information stored in the electronic record.

2 & 3: Usability and Accessibility

- 6.0.2.2.1 - The voting station shall be capable of showing the information on the paper in specific font sizes and ranges...
- 6.0.2.2.2 - The paper and electronic records shall be presented so as to allow for easy, simultaneous comparison...
- 6.0.2.3.1 - The voting station shall display, print, and store a paper record in any of the alternative languages chosen for making ballot selections...
- 6.0.2.3.2 - If the normal procedure includes VVPAT, the accessible voting station shall provide features that enable voters who are blind to perform this verification. **Note: this verification should not violate the security properties of the IDV approach, e.g., if the verification is indirect, it must be performed on equipment that is functionally separate from the voting system**

4: Approve or Spoil

6.0.2.4.1 - The voting station shall, in the presence of the voter, mark the paper record as being accepted by the voter or spoiled.

6.0.2.4.2 - The voting station shall **also** mark and preserve electronic and paper records that have been spoiled...

6.0.2.4.3 - In case of conditions that prevent voter review of the paper record, there shall be a means for the voter to notify an election official...

6.0.2.4.4 - Procedures by which election officials can be notified and prescribed actions can be taken to address discrepancies if a voter indicates that the electronic and paper records do not match shall be documented.

4: Approve or Spoil (cont)

6.0.2.4.5 - The voting station *should* not record the electronic record as being approved by the voter until the paper record has been stored.

6.0.2.4.6 - There shall be a capability to address situations in which an electronic or paper record has been recorded, approved, and stored without the intention of the voter... (e.g., due to voter error or machine error)

6.0.2.4.7 - Vendor documentation...

5: Privacy

- 6.0.2.5.1 - The privacy and anonymity of the voter's verification of his or her ballot choices on the electronic and paper records shall be maintained.
- 6.0.2.5.2 - The electronic and paper records shall be created and stored in ways that preserve the privacy and anonymity of the voter.
- 6.0.2.5.3 - The privacy and anonymity of voters whose paper records contain any of the alternative languages chosen for making ballot selections shall be maintained.
- 6.0.2.5.4 - The voter shall not be able to leave the voting area with the paper record if the information on the paper record can **directly** reveal the voter's choices.

5: Privacy (cont)

6.0.2.5.5 - Information for the purposes of auditing the electronic or paper records that may permit a voter to reveal his or her ballot choices shall be displayed so as not to be memorable by the voter.

6.0.2.5.6 – **For those voting stations that require manual handling of paper:** The privacy and anonymity of voters unable to manually handle paper and who use an accessible voting station that requires manual storage of the paper record into a ballot box shall be maintained.

6: Record Auditability

- 6.0.2.6.1 - All cryptographic software shall have been approved by the U.S. Government's Crypto Module Validation Program as applicable.
- 6.0.2.6.2 - The electronic and paper records shall include information about the election... **and the specific voting system**
- 6.0.2.6.3 - The electronic and paper records shall be linked by including a unique identifier...
- 6.0.2.6.4 - The voting station shall generate and store a digital signature for each electronic record.
- 6.0.2.6.5 - The electronic records shall be able to be exported for auditing or analysis on standards based and/or COTS information technology computing platforms...

6: Record Auditability (cont)

- 6.0.2.6.6 - The paper records should be created in a format that may be made available across different manufacturers of electronic voting systems.
- 6.0.2.6.7 - The paper record shall be created such that its contents are machine-readable...
- 6.0.2.6.8 - Any automatic accumulation of electronic or paper records shall be capable of detecting and discarding duplicate copies of the records
- 6.0.2.6.9 - The voting station should be able to print a barcode with each paper record to contain the human readable contents of the paper record and digital signature information...
- 6.0.2.6.10 - The voting system vendor shall provide full documentation of procedures for exporting its electronic records and reconciling its electronic records with its paper records.

7: Equipment

- 6.0.2.7.1 - The voting station shall be physically secure from tampering, including intentional damage...
- 6.0.2.7.2 - The voting station's printer shall be highly reliable, and easily maintained...
- 6.0.2.7.3 - Protective coverings intended to be transparent on voting station devices shall be maintainable via a predefined cleaning process. If the coverings become damaged such that they obscure the paper record, they shall be replaced.
- 6.0.2.7.4 - The paper record shall be sturdy, clean, and of sufficient durability to be used for manual auditing, machine auditing, and recounts conducted manually and via machine reading equipment...

VVPAT Requirements Discussion